JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Decentralized ChatApplication using Blockchain Technology

Keshav Khalkar, Nikhil Dhake, Sarwesh Kelzarkar, Tejas Shinde

Prof. Swapnali R. Bhujbal

P K Technical College of Engineering, gate no 714, Kadachiwadi, Chakan, Pune-4105501

Computer Department Savitribai Phule Pune University.

***Abstract*— Decentralized application make use of peer-to-peer networks, this ensures that no network failure can occur due to central node failure .This project aims to develop a decentralized chat application using blockchain technology. The application leverages the decentralized and transparent nature of blockchain to provide users with a secure and user-controlled communication platform. The use of cryptographic techniques ensures message integrity and confidentiality, allowing users to exchange messages in a secure manner. Smart contracts deployed on the blockchain enable advanced functionalities such as automated moderation, reputation systems, and decentralized file storage. The project focuses on user adoption and interface design to provide a seamless and intuitive user experience. By harnessing the power of blockchain, the decentralized chat application offers enhanced privacy, security, and control over communication activities in the digital realm.**

***Keywords*— Blockchain ,Smart Contract, peer-to-peer network**

I. INTRODUCTION

In today's generation chatting over messaging platforms are a part of an individual's lifestyle. Today's most of the communication happens over social media platforms. All these platforms also provide users the option to share multimedia attachments leveraging their communication protocols over sockets. All these chat or messaging platforms are processed through centralized servers. All the user's message or information (maybe confidential) is being processed by the central server before transmitting the same to intended recipients. The issue with these kinds of system is that all the information are visible at processing servers even if the messages or information transmitted are claimed to be end to end encrypted. The author has created a messaging or rather say a simple chat application and has explained experimentally shown how the transmitted messages are visible at processing servers. Nevertheless, the system of the centralized system has scalability issues when compared to decentralized computing systems. In this work, the author has proposed a blockchain based solution based on ethereum platform using Whisper Protocol to the issues that exist in traditional messaging or chat applications.

Introduction:

The emergence of blockchain technology has sparked a wave of innovation, enabling decentralized applications across various industries. In the realm of communication, traditional centralized chat applications have long been the norm, but they suffer from limitations such as security vulnerabilities, lack of privacy, and reliance on central servers. In contrast, decentralized chat applications leveraging blockchain technology offer a promising alternative by providing enhanced security, privacy, and user control.

The goal of this project is to develop a decentralized chat application that leverages the power of blockchain technology to create a secure and transparent messaging platform. By utilizing a distributed ledger, the application aims to eliminate the need for central intermediaries and provide users with direct control over their communication.

The decentralized nature of blockchain technology ensures that messages are not controlled or censored by any central authority, enhancing user privacy and freedom of expression. Each user maintains their private key, which serves as their digital identity and enables secure message exchange. Messages are stored on the blockchain in a transparent and tamper-resistant manner, ensuring integrity and accountability.To address the challenges of scalability, latency, and user experience, the project explores various blockchain platforms and consensus algorithms. The aim is to find the most suitable technology stack that can provide efficient and seamless communication while maintaining the benefits of decentralization.

In addition to basic messaging functionalities, the decentralized chat application may incorporate advanced features such as user profiles, group chats, and multimedia messaging. Smart contracts deployed on the blockchain can enable automated moderation, reputation systems, and decentralized file storage, further enhancing the user experience and functionality.

Throughout the project, a comprehensive analysis of potential security threats and corresponding countermeasures will be conducted to safeguard user privacy and prevent malicious activities. The application will undergo rigorous testing and evaluation to ensure its robustness and reliability in real-world scenarios.

The proposed decentralized chat application has the potential to revolutionize the way people communicate by offering a secure, transparent, and user-controlled messaging platform. By leveraging blockchain technology, this project aims to contribute to the advancement of decentralized applications and empower users with increased privacy, security, and control over their communication

decentralized chat application envisions the utilization of smart contracts deployed on the blockchain. These smart contracts can introduce advanced functionalities to enhance the user experience and provide additional capabilities. For instance, automated moderation algorithms can be implemented through smart contracts to detect and filter out inappropriate or malicious content, ensuring a safer and more pleasant communication environment.

Moreover, reputation systems can be integrated to establish trust among users by assigning reputation scores based on their behavior and interactions within the chat application. This helps users make informed decisions when engaging in conversations and fosters a positive and reliable community.

The decentralized nature of the chat application also opens up opportunities for decentralized file storage. By utilizing distributed file storage systems or interplanetary file systems (IPFS), users can securely share files, images, and other media directly within the chat application, without relying on centralized servers. This not only promotes data sovereignty but also increases the efficiency of file sharing and reduces dependency on traditional hosting services.

It is worth noting that the success of the decentralized chat application relies on adoption and user engagement. To encourage adoption, the user interface and experience should be intuitive and user-friendly, ensuring that users can seamlessly navigate the decentralized environment without prior technical knowledge of blockchain technology. Efforts should be made to educate and onboard users to understand the benefits and advantages of decentralized communication, fostering a community of empowered and informed users.

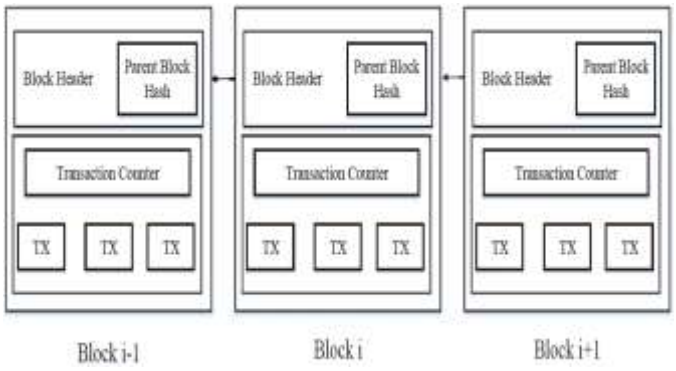


Figure 1.1 Decentralized Application Structure

Decentralized Application consists of multiple nodes connected to each other in a mesh topology type network. They are connected to each other in a Peer-to-Peer fashion. Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger.

The four main components of any blockchain ecosystemare as follows:

1. a node application
2. a shared ledger
3. a consensus algorithm
4. a virtual machine

- Node Application

Each Internet-connected computer needs to install and run a computer application specific to the ecosystem they wish to participate in. Using the case of Bitcoin as an example ecosystem, each computer must be running the Bitcoinwallet application.

- Shared Ledger

This is a logical component. The distributed ledger is a data structure managed inside the node application. Once you have the node application running, you can view the respective ledger (or blockchain) contents for that ecosystem.

- Consensus Algorithm

This, too, is a logical component of the ecosystem. The consensus algorithm is implemented as part of the node application, providing the _rules of the game‘ for how the ecosystem will arrive at a single view of the ledger.

- Virtual Machine

The virtual machine is the final logical component implemented as part of the node application that every participant in the ecosystem runs. To understand the capabilities added to an ecosystem by including a virtual machine let‘s take a quick look at what a virtual machine

LITERATURE SURVEY:

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) [2]:This seminal paper introduced the concept of blockchain technology through the creation of Bitcoin. It outlines the decentralized electronic cash system that enables secure peer-to-peer transactions without the need for intermediaries. The paper describes the proof-of-work consensus algorithm and the mechanisms to prevent double-spending, laying the foundation for blockchain-based cryptocurrencies.

Judmayer, Aljosha, et al. "Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms" (2017) [3]:This paper provides a technical overview of blockchain technology, focusing on Bitcoin and its consensus

mechanisms. It explores the concepts of cryptographic currencies, consensus ledgers, and the challenges and opportunities in the field of digital asset management. The paper also discusses Bitcoin's usability, privacy, and security challenges, highlighting the role of blockchain in shaping the future of banking and financial institutions.

Zheng, Zibin, et al. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" (2017) [4]:This paper presents an overview of blockchain architecture and compares various consensus algorithms used in different blockchain implementations. It discusses the applications of blockchain in diverse fields such as financial services, reputation systems, and the Internet of Things (IoT). The paper also highlights the technical challenges, including scalability and security, and provides insights into recent advances and future trends in blockchain technology.

Swan, Melanie. "Blockchain: Blueprint for a New Economy" (2015):In this book, Swan provides a comprehensive introduction to blockchain technology, covering its fundamental concepts, applications, and potential impact on various industries. It explores the decentralized nature of blockchain, smart contracts, and the potential for transforming finance, supply chain management, and other sectors. The book also delves into the challenges and limitations of blockchain technology.

Tapscott, Don, and Alex Tapscott. "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World" (2016):This book offers an extensive exploration of blockchain's transformative potential in various industries. It explains the underlying principles of blockchain technology and its impact on trust, transparency, and governance. The authors discuss real-world use cases, including finance, healthcare, supply chain, and energy, and provide insights into the challenges and opportunities presented by blockchain.

METHODOLOGY:

A chat application using blockchain technology leverages the inherent properties of blockchain, such as decentralization, immutability, and transparency, to provide secure and private communication between users. Here's a brief description of how such a chat application might work:

Decentralized Network: The chat application operates on a decentralized network, where multiple nodes (computers) participate in maintaining the network. This decentralization ensures that there's no central authority or single point of failure, making the chat application resilient and resistant to censorship or data manipulation.

User Identity and Authentication: Each user has a unique digital identity, represented by a cryptographic key pair. The public key is visible to other users, allowing them to verify the identity of the message sender. Users can authenticate themselves using their private keys, ensuring that only authorized individuals can access and send messages.

Message Encryption: To ensure privacy, messages sent through the chat application are encrypted using cryptographic algorithms. Only the intended recipient possessing the corresponding private key can decrypt and read the message. This encryption protects the content of the communication from unauthorized access.

Blockchain Storage: Instead of storing chat messages on a centralized server, the chat application utilizes a blockchain as a distributed ledger. Each message is treated as a transaction and added to a block. The blocks are cryptographically linked, creating an immutable chain of messages. This ensures that messages cannot be altered or tampered with once they are added to the blockchain.

Message Validation: Before a message is added to the blockchain, it goes through a validation process performed by the network nodes. Consensus algorithms, such as proof-of-work or proof-of-stake, are used to validate and agree on the order of messages, ensuring the integrity and consistency of the chat history.

Transparency and Auditability: The blockchain's transparent nature allows users to independently verify the integrity of the chat history. Any user can access the blockchain and view the entire transaction history, ensuring trust and accountability in the communication process.

Incentive Mechanism: To incentivize network participants to maintain the blockchain, a reward mechanism can be implemented. For example, in a proof-of-work system, participants who validate and add blocks to the blockchain can earn cryptocurrency as a reward, motivating them to contribute their computing power and resources.

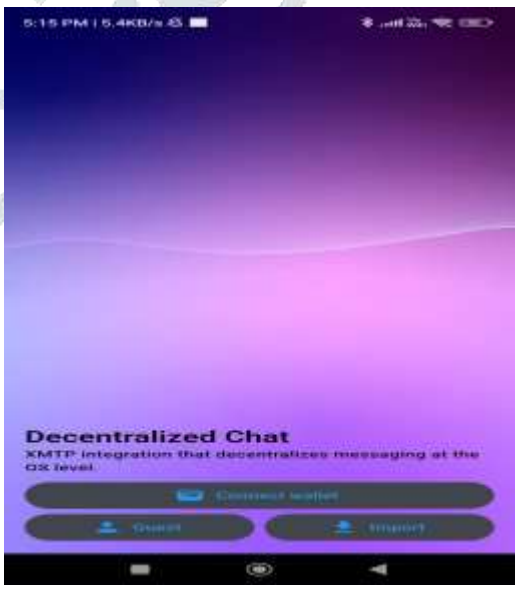
RESULT AND DISUSSION:

A).When User Open App

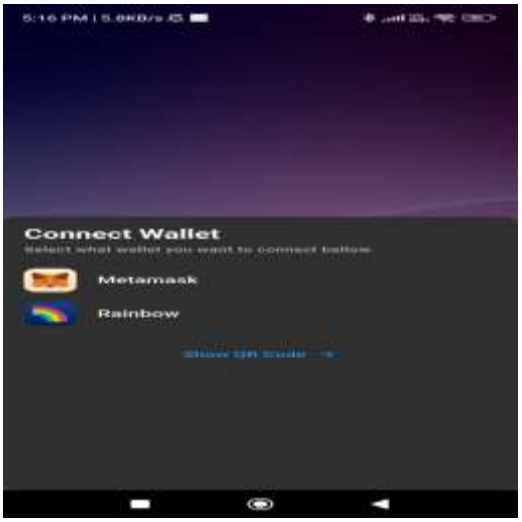
Import: We enter private key manually.

Guest: we enter as guest

Connect Wallet: Connect With the help of crypto wallets

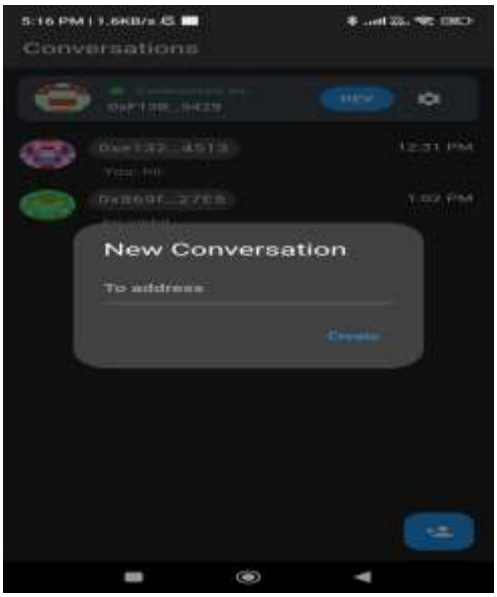


B).When User Connect With Crypto Wallet

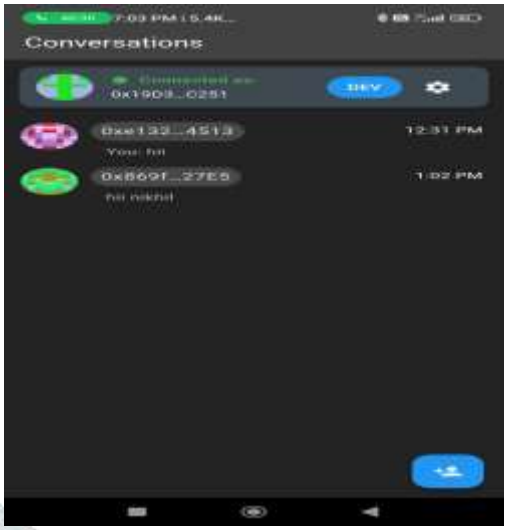


C).We Scan QR to Login To Our App

D).We Create new conversation with public Key or Wallet Address



E).When User Starts Conversation With Multiple Other Users



CONCULISON

Decentralized chat applications using blockchain technology provide secure and transparent communication channels. They offer increased user control, privacy, and accountability. By leveraging cryptographic techniques and smart contracts, these applications ensure message integrity, automate moderation, and enable decentralized file storage. While challenges remain, the potential for transforming communication and fostering user empowerment is significant..

- REFERENCES

[1] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System." March 2009.
[2] Ridhanshi Bhatia, Praveen Kumar, Shilpi Bansal and Seema Rawat. "BLOCKCHAIN –THE TECHNOLOGY OF CRYPTO CURRENCIES." In ICACCE-2018.
[3] XIAO FAN LIU, XIN-JIAN JIANG2, SI-HAO LIU AND CHI KONG TSE. "Knowledge Discovery in Cryptocurrency Transactions: A Survey". In Digital Object Identifier 10.1109/ACCESS.2021.3062652.
[4] Vaibhav Shakya, PVGN Pavan Kumar, Lakshay Tewari and Pronika. "Blockchain based Cryptocurrency Scope in India." IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2. (ICICCS 2021)
[5] FAIJAN AKHTAR, JIAN PING LI, MD BELAL BIN HEYAT, SYED LUQMAN QUADRI, SHAIK SOHAIL AHMED, XIAO YUN, AMIN UL HAQ. "POTENTIAL OF BLOCKCHAIN TECHNOLOGY IN DIGITAL CURRENCY: A REVIEW." 978-1-7281-4242-5/19/$31.00 ©2019 IEEE.
[6] Suman Ghimire and Dr. Henry Selvaraj. "A Survey on Bitcoin Cryptocurrency and its Mining." 978-1-5386-7834-3/18/$31.00 ©2018 IEEE.
[7] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks. "A Brief Survey of Cryptocurrency Systems." white paper 2016.
[8] Jae Min Kim, Jae Won Lee, Kyungsoo Lee and Junho Huh. "Proof of Phone:A Low-cost Blockchain Platform" Self-published.
[9] Yong Yuan and Fei-Yue Wang. "Blockchain and Cryptocurrencies: Model, Techniques, and Applications" 2168-2216-2018 IEEE.
[10] Wenzheng Li and Mingsheng He. "Comparative Analysis of Bitcoin, Ethereum, and Libra" 978-1-7281-6579-0/20/$31.00©2020 IEEE.
[11] Antea Knezevic, Zvonimir Musa and Tihana Babic. "Cryptocurrency as the currency of the future: a case study among ALgebra University College students." MIPRO 2020, September 28 - October 02, 2020, Opatija, Croatia.

[12] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten.
"SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies"
2015 IEEE Symposium on Security and Privacy. DOI 10.1109/SP.2015.14.
[13] Dr. R. Raju, M. SaiVignesh and K. Infant Arun Prasad. "A Study of Current Cryptocurrency Systems"
In 2018 INTERNATIONAL CONFERENCE ON COMPUTATION OF POWER, ENERGY, INFORMATION AND COMMUNICATION (ICCPEIC).
978-1-5386-2447-0/18/$31.00 ©2018 IEEE.
[14] CHANDRAMOULI SUBRAMANIAN,ASHA A GEORGE,ABHILASH K A AND MEENA KARTHIKEYAN."BLOCKCHAIN TECHNOLOGY BOOK".
[15]"ONLINE PAYMENT USING BLOCKCHAIN" RESEARCH PAPER.